UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/046,819	01/17/2002	Takuya Kobayashi	2002_0037A	5356

513 7590 05/16/2005

WENDEROTH, LIND & PONACK, L.L.P.
2033 K STREET N. W.
SUITE 800
WASHINGTON, DC 20006-1021

EXAMINER	
CERVETTI, DAVID GARCIA	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 05/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/046,819	**Applicant(s)** KOBAYASHI ET AL.	
	Examiner David G. Cervetti	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 January 2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *3/4/04,9/17/03*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Drawings

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: S206, S209 (Figure 20), 292 (Figure 22). Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

2. The disclosure is objected to because of the following informalities: "I/O" (page 1, line 22). While well known in the art, these terms have not been defined.

3. The disclosure is objected to because of the following informalities: "no authorized user should not be allowed to access such personal information", perhaps "unauthorized" was intended. Appropriate correction is required.

4. The disclosure is objected to because of the following informalities: "in fig 23, an unprotectedTag tag 295", perhaps "in fig 22" was intended. Appropriate correction is required.

Claim Objections

5. Claim 13 is objected to because of the following informalities: "date processor" (page 64, line 2 of the claim); perhaps "data processor" was intended. Appropriate correction is required.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

7. Claims 1-19 are rejected under 35 U.S.C. 102(a) as being anticipated by Woolsey et al. (US Patent Number: 6,029,000).

Regarding claim 1, Woolsey et al. teach a data processor comprising:

- transmission/reception means for transmitting/receiving data to/from a server connected over a network (figure 5, column 19, lines 14-28);
- validity determination means for determining whether said command data is valid (figure 6, column 20, lines 50-67, column 21, lines 1-17);
- command data processing means for retrieving, when said command data is determined as valid by said validity determination means, the data component specified by said command data from said server using

said transmission/reception means (figure 6, column 20, lines 50-67, column 21, lines 1-17); and

- data component processing means for controlling said data processor based on the data component retrieved by said command data processing means (column 22, lines 50-60).

Regarding claim 2, Woolsey et al. teach wherein said data component processing means performs screen display based on the data component retrieved by said command data processing means (column 19, lines 47-67, column 20, lines 13-47).

Regarding claim 3, Woolsey et al. teach wherein said data component processing means outputs the data component retrieved by said command data processing means to outside of said data processor (column 19, lines 47-63).

Regarding claim 4, Woolsey et al. teach wherein the data component used for controlling said data processor by said data component processing means is limited to be the data component retrieved by said command data processing means (column 3, lines 65-67, column 4, lines 1-11).

Regarding claim 5, Woolsey et al. teach wherein said command data is encrypted, and said validity determination means determines whether said command data is valid after decrypting the same (column 20, lines 50-67, column 21, lines 1-17).

Regarding claim 6, Woolsey et al. teach wherein said command data processing means determines whether the data component retrieved from said server is valid, and if determined valid, supplies the data component to said data component processing means (column 20, lines 50-67, column 21, lines 1-17).

Regarding claim 7, Woolsey et al. teach wherein said command data processing means includes a language processing section for interpreting a JAVA language, and a JAVA applet to be processed by said language processing section (column 19, lines 15-67, column 20, lines 13-47).

Regarding claim 8, Woolsey et al. teach wherein said transmission/reception section receives, in accordance with a user's instruction, the JAVA applet included in said command data processing means (column 19, lines 15-67, column 20, lines 13-47).

Regarding claim 9, Woolsey et al. teach wherein said transmission/reception means receives, in accordance with a user's instruction, said command data for supply to said validity determination means (column 20, lines 50-67, column 21, lines 1-17).

Regarding claim 10, Woolsey et al. teach a data processor comprising:

- transmission/reception means for transmitting/receiving data to/from a server connected over a network (figure 5, column 19, lines 14-28);
- validity determination means for determining whether said command data is valid (figure 6, column 20, lines 50-67, column 21, lines 1-17);
- command data processing means for retrieving, when said command data is determined as valid by said validity determination means, the data component included in said command data (figure 6, column 20, lines 50-67, column 21, lines 1-17); and

- data component processing means for controlling said data processor based on the data component retrieved by said command data processing means (column 22, lines 50-60).

Regarding claim 11, Woolsey et al. teach wherein said data component processing means performs screen display based on the data component retrieved by said command data processing means (column 19, lines 47-67, column 20, lines 13-47).

Regarding claim 12, Woolsey et al. teach wherein said data component processing means outputs the data component retrieved by said command data processing means to outside of said data processor (column 19, lines 47-63).

Regarding claim 13, Woolsey et al. teach wherein the data component used for controlling said date processor by said data component processing means is limited to be the data component retrieved by said command data processing means (column 3, lines 65-67, column 4, lines 1-11).

Regarding claim 14, Woolsey et al. teach wherein said command data is encrypted, and said validity determination means determines whether said command data is valid after decrypting the same (column 20, lines 50-67, column 21, lines 1-17).

Regarding claim 15, Woolsey et al. teach wherein said command data processing means includes a language processing section for interpreting a JAVA language, and a JAVA applet to be processed by said language processing section (column 19, lines 15-67, column 20, lines 13-47).

Regarding claim 16, Woolsey et al. teach wherein said transmission/reception section receives, in accordance with a user's instruction, the JAVA applet included in said command data processing means (column 19, lines 15-67, column 20, lines 13-47).

Regarding claim 17, Woolsey et al. teach wherein said transmission/reception means receives, in accordance with a user's instruction, said command data for supply to said validity determination means (column 20, lines 50-67, column 21, lines 1-17).

Regarding claim 18, Woolsey et al. teach

- a transmission/reception step of transmitting/receiving data to/from a server connected over a network (figure 5, column 19, lines 14-28);
- a validity determination step of determining whether said command data is valid (figure 6, column 20, lines 50-67, column 21, lines 1-17);
- a command data processing step of retrieving, when said command data is determined as valid in said validity determination step, the data component specified by said command data from said server by calling for said transmission/reception step (figure 6, column 20, lines 50-67, column 21, lines 1-17); and
- a data component processing step of controlling said data processor based on the data component retrieved in said command data processing step (column 22, lines 50-60).

Regarding claim 19, Woolsey et al. teach

- a transmission/reception step of transmitting/receiving data to/from a server connected over a network (figure 5, column 19, lines 14-28);
- a validity determination step of determining whether said command data is valid (figure 6, column 20, lines 50-67, column 21, lines 1-17);
- a command data processing step of retrieving, when said command data is determined as valid in said validity determination step, the data component included in said command data (figure 6, column 20, lines 50-67, column 21, lines 1-17); and
- a data component processing step of controlling said data processor based on the data component retrieved in said command data processing step (column 22, lines 50-60).

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. Claims 24-25 are rejected under 35 U.S.C. 102(e) as being anticipated by Kolouch (US Patent Number: 6,694,433).

Regarding claim 24, Kolouch teaches a data processing method for receiving and processing data to which information for tampering detection is added, said method comprising:

- a reception step of receiving data which includes an authentication information region for including the tampering detection information, a protected data region for including data to be subjected to tampering detection, and an unprotected data region for including data not to be subjected to tampering detection, wherein said protected data region includes an unprotection list which lists, by type, the data included in said unprotected data region (column 4, lines 53-67, figure 5, column 5, lines 1-49);
- a protected data authentication step of detecting, for the data received in said reception step, whether the data included in said protected data region has been tampered by using the tampering detection information included in said authentication information region (column 4, lines 53-67, figure 5, column 5, lines 1-49); and
- an unprotected data authentication step of authenticating, for the data received in said reception step, whether the data included in said unprotected data region is valid based on said unprotection list which has been confirmed as not having been tampered in said protected data authentication step (column 4, lines 53-67, figure 5, column 5, lines 1-49).

Regarding claim 25, Kolouch teaches a data processing method for transferring data to which information for tampering detection is added from a transmitting data processor to a receiving data processor, wherein

- said transmitting data processor performs:
- an unprotection list generation step of generating an unprotection list which lists, by type, data not to be subjected to tampering detection (column 4, lines 53-67, figure 5, column 5, lines 1-49);
- a data generation step of generating data to be transmitted by arranging data to be subjected to tampering detection in a protected data region together with said unprotection list, the data not to be subjected to tampering detection in an unprotected data region, and the tampering detection information derived based on the data in said protected data region in an authentication information region (column 4, lines 53-67, figure 5, column 5, lines 1-49); and
- a transmission step of transmitting the data generated in said data generation step (column 4, lines 53-67, figure 5, column 5, lines 1-49), and
- said receiving data processor performs:
- a reception step of receiving the data transmitted from said transmitting data processor (column 4, lines 53-67, figure 5, column 5, lines 1-49);
- a protected data authentication step of detecting, for the data received in said reception step, whether the data in said protected data region has

been tampered by using the tampering detection information in said authentication information region (column 4, lines 53-67, figure 5, column 5, lines 1-49); and

- an unprotected data authentication step of authenticating, for the data received in said reception step, whether the data included in said unprotected data region is valid based on said unprotection list which has been confirmed as not having been tampered in said protected data authentication step (column 4, lines 53-67, figure 5, column 5, lines 1-49).

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 20-23, 26-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Woolsey et al., and further in view of Kolouch.

Regarding claim 20, Woolsey et al. teach the features of digital signing and encryption (column 20, lines 50-67, column 21, lines 1-17). Woolsey et al. do not expressly disclose protected and unprotected data regions. However, Kolouch teaches a data processor comprising:

- reception means for receiving data which includes an authentication information region for including the tampering detection information, a protected data region for including data to be subjected to tampering detection, and an unprotected data region for including data not to be subjected to tampering detection, wherein said protected data region includes an unprotection list which lists, by type, the data included in said unprotected data region (column 4, lines 53-67, figure 5, column 5, lines 1-49);
- protected data authentication means for detecting, for the data received by said reception means, whether the data included in said protected data region has been tampered by using the tampering detection

information included in said authentication information region (column 4, lines 53-67, figure 5, column 5, lines 1-49); and

- unprotected data authentication means for authenticating, for the data received by said reception means, whether the data included in said unprotected data region is valid based on said unprotection list which has been confirmed as not having been tampered by said protected data authentication means (column 4, lines 53-67, figure 5, column 5, lines 1-49).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to send protected and unprotected data regions. One of ordinary skill in the art would have been motivated do so to provide a more granular access control (Kolouch, column 5, lines 60-67).

Regarding claim 21, the combination of Woolsey et al. and Kolouch teaches the limitations as set forth under claim 20 above. Furthermore, Kolouch teaches wherein the data received by said reception means is hypertext, and said unprotection list lists, by type, a tag included in said unprotected data region (column 5, lines 13-67).

Regarding claim 22, Woolsey et al. teach the features of digital signing and encryption (column 20, lines 50-67, column 21, lines 1-17). Woolsey et al. do not expressly disclose protected and unprotected data regions. However, Kolouch teaches a data processor structured by a transmitting data processor and a receiving data processor, wherein the transmitting data processor transfers, to the receiving data processor, data to which information for tampering detection is added, wherein said transmitting data processor comprises:

- unprotection list generation means for generating an unprotection list which lists, by type, data not to be subjected to tampering detection (column 4, lines 53-67, figure 5, column 5, lines 1-49);
- data generation means for generating data to be transmitted by arranging data to be subjected to tampering detection in a protected data region together with said unprotection list, the data not to be subjected to tampering detection in an unprotected data region, and the tampering detection information derived based on the data in said protected data region in an authentication information region (column 4, lines 53-67, figure 5, column 5, lines 1-49); and
- transmission means for transmitting the data generated by said data generation means (column 4, lines 53-67, figure 5, column 5, lines 1-49), and
- said receiving data processor comprises:
- reception means for receiving the data transmitted from said transmitting data processor (column 4, lines 53-67, figure 5, column 5, lines 1-49);
- protected data authentication means for detecting, for the data received by said reception means, whether the data in said protected data region has been tampered by using the tampering detection information in said

authentication information region (column 4, lines 53-67, figure 5, column 5, lines 1-49); and

- unprotected data authentication means for authenticating, for the data received by said reception means, whether the data included in said unprotected data region is valid based on said unprotection list which has been confirmed as not having been tampered by said protected data authentication means (column 4, lines 53-67, figure 5, column 5, lines 1-49).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to send protected and unprotected data regions. One of ordinary skill in the art would have been motivated do so to provide a more granular access control (Kolouch, column 5, lines 60-67).

Regarding claim 23, the combination of Woolsey et al. and Kolouch teaches the limitations as set forth under claim 22 above. Furthermore, Kolouch teaches wherein the data generated by said data generation means is hypertext, and said unprotection list lists, by type, a tag included in said unprotected data region (column 5, lines 13-67).

Regarding claim 26, Woolsey et al. teach a data processor for receiving and processing data with a digital signature, comprising: reception means for receiving the data with the digital signature from a server connected over a network (column 20, lines 50-67, column 21, lines 1-17). Woolsey et al. do not expressly disclose signer certificate acquiring means for acquiring a signer certificate indicating, by type, what data is signable by a signer of the data received by said reception means; and signature authentication means for determining, when the signer certificate acquired by said signer certificate acquiring means indicates, by type, the data received by said reception means, that a signature applied to the data as valid. However, Kolouch teaches signer certificate acquiring means for acquiring a signer certificate indicating, by type, what data is signable by a signer of the data received by said reception means (column 4, lines 53-67, figure 5, column 5, lines 1-49); and signature authentication means for determining, when the signer certificate acquired by said signer certificate acquiring means indicates, by type, the data received by said reception means, that a signature applied to the data as valid (column 4, lines 53-67, figure 5, column 5, lines 1-49). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to determine, based on a signer certificate, what data is signable by a signer. One of ordinary skill in the art would have been motivated do so to provide a more granular access control (Kolouch, column 5, lines 60-67).

Regarding claim 27, the combination of Woolsey et al. and Kolouch teaches the limitations as set forth under claim 26 above. Furthermore, Kolouch teaches wherein said signer certificate can include, in a list, by type, a plurality of the signable data (column 5, lines 33-67).

Regarding claim 28, the combination of Woolsey et al. and Kolouch teaches the limitations as set forth under claim 26 above. Furthermore, Kolouch teaches wherein said signer certificate can include a wildcard as a type of the signable data, and when the signer certificate acquired by said signer certificate acquiring means includes the wildcard as the type of the signable data, said signature authentication means determines that the signature applied to any data received in said reception means as valid (column 5, lines 33-67, column 6, lines 1-60).

Regarding claim 29, the combination of Woolsey et al. and Kolouch teaches the limitations as set forth under claim 26 above. Furthermore, Kolouch teaches wherein said signature authentication means acquires a type of the data based on a characteristic part of a URI (Uniform Resource Identifier) of the data received by said reception means (column 5, lines 33-67, column 6, lines 1-60).

Regarding claim 30, the combination of Woolsey et al. and Kolouch teaches the limitations as set forth under claim 26 above. Furthermore, Kolouch teaches wherein said signature authentication means acquires the type of the data based on a header part of the data received by said reception means (column 5, lines 33-67, column 6, lines 1-60).

Regarding claim 31, the combination of Woolsey et al. and Kolouch teaches the limitations as set forth under claim 26 above. Furthermore, Kolouch teaches wherein said signer certificate acquiring means receives said signer certificate by using said reception means (column 5, lines 33-67, column 6, lines 1-60).

Regarding claim 32, Woolsey et al. teach a data processing method for receiving and processing data with a digital signature, comprising: a reception step of receiving the data with the digital signature from a server connected over a network (column 20, lines 50-67, column 21, lines 1-17). Woolsey et al. do not expressly disclose a signer certificate acquiring step of acquiring a signer certificate indicating, by type, what data is signable by a signer of the data received in said reception step; and a signature authentication step of determining, when the signer certificate acquired in said signer certificate acquiring step indicates, by type, the data received in said reception step, that a signature applied to the data as valid. However, Kolouch teaches a signer certificate acquiring step of acquiring a signer certificate indicating, by type, what data is signable by a signer of the data received in said reception step (column 4, lines 53-67, figure 5, column 5, lines 1-49); and a signature authentication step of determining, when the signer certificate acquired in said signer certificate acquiring step indicates, by type, the data received in said reception step, that a signature applied to the data as valid (column 4, lines 53-67, figure 5, column 5, lines 1-49). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to determine, based on a signer certificate, what data is signable by a signer. One of ordinary skill in the art would have been motivated do so to provide a more granular access control (Kolouch, column 5, lines 60-67).

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100